Indiana Intelligence Fusion Center

Privacy Policy

June 1, 2018

The Indiana Intelligence Fusion Center Privacy Policy represents the privacy policy applicable to all IIFC operations and activities.

INDIANA INTELLIGENCE FUSION CENTER
PRIVACY POLICY

Table of Contents

{Remainder of page intentionally left blank}

A. PURPOSE

The mission of the Indiana Intelligence Fusion Center (IIFC) is to collect, evaluate, analyze and disseminate information and intelligence data regarding criminal and terrorist activity in the State of Indiana while following Department of Homeland Security's (DHS) Fair Information Practice Principles (FIPPs) and 28 CFR, Part 23 to ensure the rights and privacy of individuals and organizations.

The information and intelligence data collected, evaluated, and analyzed will be disseminated by the IIFC to members of the law enforcement and public safety communities responsible for the prevention, mitigation, and response to crime and terrorism.

The IIFC recognizes the importance of ensuring the protection of individual constitutional rights, civil liberties, civil rights, and privacy interests throughout the intelligence process.

The IIFC policy manual contains the standards the IIFC will adhere to for the collection, use, and security of intelligence and information, as well as accountability guidelines for the management of such intelligence or information.

B. POLICY APPLICABILITY and LEGAL COMPLIANCE

All IIFC personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, and other authorized users will comply with the IIFC's privacy policy concerning the information the center collects, receives, maintains, archives, accesses, or discloses, or disseminates to center personnel, governmental agencies (including Information Sharing Environment (ISE) participating agencies), and participating justice and public safety agencies, as well as to private contractors and the general public.

The IIFC will provide an electronic copy of this policy to all IIFC and non-IIFC personnel via posting on the IIFC website.

All IIFC personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, agencies that originate information, and other authorized users will comply with applicable laws protecting privacy, civil rights, and civil liberties.

C. GOVERNANCE and OVERSIGHT

Primary responsibility for the operation of the IIFC, its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis destruction, sharing, or disclosure of information; and the enforcement of this policy is assigned to the Executive Director of the IIFC.

The Executive Director adheres to enforcement procedures outlined in this policy.

IIFC privacy compliance is guided by a trained Privacy Officer who is appointed by the Executive Director. Violations of the privacy policy can be reported to, the Executive Director, Assistant Director or to the Privacy Officer. Reporting can be made in person, written or via any electronic communication.

IIFC employees, contract employees and persons on assignment to the IIFC from other agencies are responsible for adhering to this policy. Failure to abide by this policy may result in disciplinary action up to and including dismissal.

D. DEFINITIONS

The primary terms and definitions used in this privacy policy are set forth in Appendix A- Definitions

E. INFORMATION

The Indiana intelligence fusion center may collect criminal intelligence information only if:

- Reasonable suspicion exists that the subject of the criminal intelligence information is involved with or has knowledge of possible criminal or terrorist activity; and
- The criminal intelligence information is relevant to the criminal or terrorist activity.

The IIFC may retain information that is based on a level of suspicion that is less than "reasonable suspicion," such as tips and leads or suspicious activity report (SAR) information, as it pertains to terrorist activity, subject to the policies and procedures specified in the ISE- SAR Functional Standard.

The IIFC will not seek or retain, and information-originating agencies will agree not to submit, information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations.

The IIFC applies labels to agency-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:

- the information pertains to all individuals pursuant to IC 10-11-9-4, and
- The information is subject to Federal and Indiana state laws restricting access, use, or disclosure, including, but not limited to, 18 USC 2721, IC 35-38-9 et seq., IC 31-39-8 et seq., IC 4-1-10 et seq., IC 5-2 et seq., IC 5-14-3 et seq., and 28 CFR, Part 23.

IIFC personnel will, upon receipt of information, assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency will assign categories to the information) to reflect the assessment, such as:

- Whether the information consists of tips and leads data, suspicious activity reports, criminal history or intelligence information, case records, conditions of supervision, or case progress, etc.;
- The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector);
- The reliability of the source (for example, reliable, usually reliable, unreliable, unknown); and
- The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

At the time a decision is made to retain information, it will be labeled (by record, data set, or system of records), to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:

- Protect confidential sources and police undercover techniques and methods;
- Not interfere with or compromise pending criminal investigations;
- Protect an individual's right of privacy, civil rights, and civil liberties; and
- Provide legally required protection based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.
- There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

IIFC personnel are required to adhere to the ISE- SAR Functional Standard and state and federal law for the receipt, collection, assessment, storage, access, dissemination, retention, and security of Suspicious activity reporting (SAR) information.

The IIFC incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as constitutional rights, including personal privacy and other civil liberties, and civil rights.

The IIFC will identify and review information that is originated by the IIFC prior to sharing that information in the ISE.

The IIFC requires certain basic descriptive information to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure. The types of information should include:

- The name of the originating department, component, and subcomponent.
- The name of the agency's justice information system from which the information is disseminated.
- The date the information was collected and, where feasible, the date its accuracy was last verified.
- The title and contact information for the person to whom questions regarding the information should be directed.

The IIFC will attach (or ensure that the originating agency has attached) specific labels and descriptive metadata to information that will be used, accessed, or disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification.

The IIFC will keep a record of the source of all information retained by the agency.

F. ACQUIRING AND RECEIVING INFORMATION

Information gathering (acquisition and access) and investigative techniques used by the IIFC and information-originating agencies are in compliance with and will adhere to applicable regulations and guidelines, including:

- 28 CFR, Part 23 regarding criminal intelligence information
- DHS' Fair Information Practice Principles (under certain circumstances, there may be exceptions to the Fair Information Practice Principles, based, for example, on authorities paralleling those provided in the federal Privacy Act; state, local, and tribal laws; or agency/center policy)
- Applicable constitutional provisions in, IC 10-11-9 et seq.

Information gathering techniques used by the IIFC will (and for originating agencies should) be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.

External agencies that access and share information with the IIFC are governed by the laws and rules governing those individual agencies, as well as by applicable federal and state laws.

The IIFC will make every effort to contract only with commercial database entities that provide an assurance that their methods for gathering personally identifiable information comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that these methods are not based on misleading information collection practices.

The IIFC will not directly or indirectly receive, seek, accept, or retain information from an individual or information provider that is legally prohibited from obtaining or disclosing the information.

G. INFORMATION QUALITY ASSURANCE

The IIFC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources of information; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard has been met.

At the time of retention in the system, the information will be labeled regarding its level of quality (accurate, complete, current, verifiable, and reliable).

The IIFC investigates, in a timely manner, alleged errors and deficiencies (or refers them to the originating agency) and corrects, deletes, or refrains from using protected information found to be erroneous or deficient.

The labeling of retained information will be reevaluated when new information is gathered that has an impact on the confidence (validity and reliability) in previously retained information.

The IIFC will make every reasonable effort to ensure that information will be corrected, deleted from the system, or not used when the agency/center learns that the information is erroneous, misleading, obsolete, or

otherwise unreliable; the source of the information did not have authority to gather the information or to provide the information to the agency; or the source used prohibited means to gather the information, except when the source did not act as an agent to a bona fide law enforcement officer.

Originating agencies external to the IIFC are responsible for the quality and accuracy of the data accessed by or provided to the IIFC. The IIFC will advise the appropriate contact person in the originating agency, in writing, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

External agencies that access and share information with the IIFC are governed by the laws and rules governing those individual agencies, as well as by applicable federal and state laws.

The IIFC will contract only with commercial database entities that provide an assurance that their methods for gathering personally identifiable information comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that these methods are not based on misleading information collection practices.

The IIFC will not directly or indirectly receive, seek, accept, or retain information from an individual or information provider that is legally prohibited from obtaining or disclosing the information

H. COLLATION AND ANALYSIS

Information acquired or received by the IIFC or accessed from other sources will be analyzed only by qualified individuals who have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly.

Information subject to collation and analysis is information as defined and identified in Section E, Information.

Information acquired or received by the IIFC or accessed from other sources is analyzed according to priorities and needs and will be analyzed only to:

- Further crime prevention (including terrorism), enforcement, force deployment, or prosecution objectives and priorities established by the IIFC, and
- Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal (including terrorist) activities.

I. MERGING RECORDS

The set of identifying information sufficient to allow merging will utilize reasonable steps to identify the subject and may include the name (full or partial) and, in most cases, one or more of the following: date of birth; law enforcement or corrections system identification number; individual identifiers, such as fingerprints, photographs, physical description, height, weight, eye and hair color, race, ethnicity, tattoos, or scars; social security number; driver's license number; or other biometrics, such as DNA, retinal scan, or facial recognition. The identifiers or characteristics that, when combined, could clearly establish that the information from multiple records is about the same organization may include the name, federal or state tax ID number, office address, and telephone number.

If the matching requirements are not fully met but there is an identified partial match, the information may be associated if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

J. SHARING AND DISCLOSURE

Credentialed, role-based access criteria will be used, as appropriate, to control:

- The information to which a particular group or class of users can have access based on the group or class;
- The information a class of users can add, change, delete, or print; and
- To whom, individually, the information can be disclosed and under what circumstances.

The IIFC adheres to national standards for the suspicious activity reporting (SAR) process, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process within the ISE that complies with the current version of the ISE-SAR Functional Standard.

Access to or disclosure of records retained by the IIFC will be provided only to persons within other governmental agencies or private sector entities who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with law and procedures applicable to the agency for which the person is working. An audit trail will be kept of access by or dissemination of information to such persons.

Agencies external to the IIFC may not disseminate IIFC information received from IIFC without approval from the originator of the information. This requirement does not apply to information that was already provided to, disclosed to, or independently acquired by, the IIFC without restrictions from its originating source. The external agencies may be required to obtain approval from the IIFC to disseminate the information received from the IIFC as needed.

Records retained by the IIFC may be accessed or disseminated to those responsible for public protection, safety, or public health only for public protection, safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. An audit trail sufficient to allow the identification of each individual who accessed or received information will be kept.

Information gathered and records retained by the IIFC may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those users and purposes specified in the law. An audit trail will be kept for a minimum of three (3) years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

Information gathered and records retained by the IIFC may be accessed or disclosed to a member of the public only if the information is defined by law to be a public record or otherwise appropriate for release to further the IIFC mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the laws of the State of Indiana for this type of information. An audit trail will be kept of all requests and of what information is disclosed to a member of the public.

Information gathered and records retained by the IIFC will not be:

- Sold, published, exchanged, or disclosed for commercial purposes;
- Disclosed or published without prior notice to the originating agency that such information is subject to re-disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency; or
- Disseminated to persons not authorized to access or use the information.

There are several categories of records that will ordinarily not be provided to the public under the Indiana Access to Public Records Act, this includes but limited to:

- Records required to be kept confidential by law are exempted from disclosure requirements under IC 5-14-3-4.
- Investigatory records of law enforcement agencies are exempted from disclosure requirements under IC 5-14-3-4 (b)(1); however, certain law enforcement records must be made available for inspection and copying under IC 5-14-3-5.
- Criminal Intelligence Information pursuant to IC 5-2-4-6 is declared criminal confidential and exempted from the Indiana Access to Public Records Act (IC 5-14-3-4(b) at the discretion of a public agency), unless, access to the records is specifically required by a state or federal statute or is ordered by a court under the rules of discovery.
- A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempted from disclosure requirements under IC 5-14-34(b)(19).
- Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot be shared without permission, unless they are required to be disclosed under the Indiana Access to Public Records Act. Participating agencies providing data remain the owners of the data contributed and, as such, are responsible for granting access when required by applicable federal or state law or court order.
- Subject only to the requirement of IIFC to comply with the Indiana Access to Public Records Act or other applicable law, the IIFC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.
- IIFC participating agencies providing data remain the owners of the data contributed to the IIFC. The IIFC may be required by statute, regulation, or mutual agreement, to use or disseminate the data in a particular manner. Members of the public can access individually identifiable information on themselves from the IIFC, as permissible by law, by making a request under the Indiana Access to

Public Records Act or other law permitting access, or by making a request to the originating agency. Persons wishing to access data pertaining to themselves should communicate directly with the agency or entity that is the source of the data. Citizen inquiries to the IIFC about personal data are the responsibility of the Indiana State Police Legal Department. The IIFC Assistant Director will notify the agency who is the owner or originator of the data of the request. The agency shall designate in writing to the IIFC which of those records, if any, the agency considers confidential information or otherwise exempted from disclosure under exceptions to the Indiana Access to Public Records Act set forth in IC 5-14-34. The IIFC shall promptly review the basis for the agency's claims, including claims of confidentiality under federal laws, and shall not disclose the records subject to the agency's claims if the IIFC concurs with the agency's claims. If the IIFC determines that its obligations under the Indiana Access to Public Records Act requires such disclosure, the IIFC shall promptly notify the agency of such determination and will not make such disclosure if the agency obtains, prior to the expiration of the applicable timeframe to respond to such request, either an opinion from the Indiana Public Access Counselor that such disclosure is not required, or a protective order or other relief from any court of competent jurisdiction preventing such disclosure. This must be done in sufficient time to permit IIFC compliance with deadlines found with IC 5-14-3-9.

- Participating agencies agree that they will notify owners of the information of requests related to individually identifiable information.
- Upon receipt of a request for one or more documents under the Indiana Access to Public Records Act, IIFC personnel will immediately contact an attorney in the Indiana State Police Legal Department for assistance in responding to the request. A prompt response is required under Indiana Law, with very short deadlines which vary depending upon the circumstances of the request for records.

K. REDRESS

K.1 Disclosure

Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity.

An individual is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the IIFC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The IIFC's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual.

Pursuant to the IIFC's lawful discretion, the existence, content, and source of the information will not be made available to an individual, unless required under the Indiana Access to Public Records Act or other law, when:

- Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution;
- Disclosure would endanger the health or safety of an individual, organization, or community;
- The information is in a criminal intelligence system;
- The information is classified under federal law.
- The information source does not reside with the IIFC; or

- The IIFC did not originate or does not have a right to disclose the information.

If the information does not originate with the entity, the requestor will be referred to the originating agency.

K.2 Complaints and Corrections

If an individual has complaints or objections to the accuracy or completeness of information about him or her originating with the IIFC, including information that may be shared through the ISE, the IIFC's Privacy Officer or legal counsel will inform the individual of the procedure for submitting complaints or requesting corrections. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

If an individual has complaints or objections to the accuracy or completeness of information about him or her that originates with another agency, including information that is shared through the ISE, the Privacy Officer or legal counsel will notify the originating agency of the complaint or request for correction and coordinate with the originating agency to assist the individual with complaint and corrections procedures. A record will be kept of all such complaints and requests for corrections and the resulting action taken, if any.

If an individual has a complaint or objection to the accuracy or completeness of terrorism-related information that has been or may be shared through the ISE that: (a) is held by the IIFC; (b) allegedly resulted in harm to the complainant; and (c) is exempt from disclosure, the IIFC will inform the individual of the procedure for submitting (if needed) and resolving complaints or objections. Complaints should be directed to the IIFC Privacy Officer at the following e-mail address: iifc@iifc.in.gov. The IIFC will acknowledge the complaint and state that it will be reviewed, but will not confirm the existence of the information that is exempt from disclosure, as permitted by law. If the information did not originate with the IIFC, IIFC will notify the originating agency in writing and, upon request, assist such agency to correct or purge any identified data/record deficiencies, subject to applicable records retention procedures, or to verify that the record is accurate. Any personal information originating with the IIFC will be reviewed and corrected in or deleted from IIFC data/records according to applicable records retention procedures if it is determined to be erroneous, include incorrectly merged information, or out of date. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

An individual to whom information has been disclosed will be given reasons if requests for correction(s) are denied by the IIFC or originating agency, including ISE participating agencies, and be informed of any existing procedure for appeal.

To delineate protected information shared through the ISE from other data, the IIFC maintains records of agencies sharing terrorism-related information and audit logs and employs system mechanisms to identify the originating agency when the information is shared.

L. SECURITY SAFEGUARDS

The IIFC Director of Operations is designated and trained to serve as the IIFC's Security Officer.

The IIFC will operate in a secure facility protecting the facility from external intrusion. The IIFC will utilize secure internal and external safeguards against network intrusions. Access to IIFC databases from outside the facility will be allowed only over secure networks.

The IIFC will secure tips, leads, and ISE-SAR information in the same system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.

Queries made to the IIFC data applications will be logged into the data system identifying the user initiating the query.

The IIFC will utilize watch logs to maintain audit trails of requested and disseminated information.

To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

The IIFC will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.

Access to IIFC information will be granted only to IIFC personnel whose positions and job duties require such access; who have successfully completed a background check and appropriate security clearance, if applicable; and who have been selected, approved, and trained accordingly.

The IIFC will notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the person. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release.

The IIFC will immediately notify the originating agency from which the entity received personal information of a suspected or confirmed breach of such information.

M. INFORMATION RETENTION AND DESTRUCTION

All identified person or organization information will be reviewed for record retention (validation or purge) at least every five (5) years, as provided by 28 CFR Part 23, or a shorter period specified by state or local law.

When information has no further value or meets the criteria for removal according to the IIFC's retention and destruction policy or according to applicable law, it will be purged, destroyed, and deleted or returned to the submitting source.

The IIFC will delete information or return it to the source unless it is validated, as specified in 28 CFR Part 23.

Notification of proposed destruction or return of records may or may not be provided to the source agency, depending on the relevance of the information and any agreement with the providing agency.

N. ACCOUNTABILITY AND ENFORCEMENT

N.1 Information System Transparency

The IIFC will be open with the public in regard to information and intelligence collection practices. The IIFC privacy policy will be posted to the IIFC's website.

The IIFC's Privacy Officer will be responsible for responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s).

N.2 Accountability

The audit log of queries made to the IIFC will identify the user initiating the query.

The IIFC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for a minimum of three (3) years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

The IIFC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with their systems, in provisions of this policy and applicable law. This will include logging access of these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits will be mandated at least quarterly, and a record of the audits will be maintained by the Deputy Director of Operations of the agency.

The IIFC's personnel or other authorized users shall report violations or suspected violations of agency/center policies relating to protected information to the IIFC Privacy Officer or Executive Director or Assistant Director.

The IIFC will annually conduct an audit and inspection of the information contained in its criminal intelligence system. This auditor has the option of conducting a random audit, without announcement, at

any time and without prior notice to the IIFC. This audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the center's criminal intelligence systems.

The Privacy Officer, will review and update the provisions protecting privacy, civil rights, and civil liberties contained within this policy annually and will make appropriate changes in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations.

N.3 Enforcement

If IIFC personnel, personnel assigned to the IIFC from a participating agency, contractor, or any user of IIFC is found to be in noncompliance with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, the Executive Director of the IIFC will:

- Suspend or discontinue access to information by the user;
- Suspend, demote, transfer, or terminate the person, as permitted by applicable personnel policies;
- Apply administrative actions or sanctions as provided by state police rules and regulations or as provided in agency/center personnel policies;
- If the user is from an agency external to the agency, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions; or
- Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

The IIFC reserves the right to restrict the qualifications and number of personnel having access to IIFC information and to suspend or withhold service to any personnel violating the privacy policy. The IIFC reserves the right to deny access to any participating agency user who fails to comply with the applicable restrictions and limitations of the IIFC's privacy policy.

O. TRAINING

The IIFC will require all assigned personnel of IIFC to participate in training programs regarding implementation of and adherence to the IIFC's privacy, civil rights, and civil liberties policy

All personnel assigned to the IIFC shall be required to annually take 28 CFR part 23 training.

The IIFC will provide special training to personnel authorized to share protected information through the ISE regarding the IIFC requirements and policies for collection, use, and disclosure of protected information.

The IIFC privacy policy training program will cover:

- Purposes of the privacy, civil rights, and civil liberties protection policy;
- Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the IIFC;
- How to implement the policy in the day-to-day work of the user, whether a paper or systems user;
- The impact of improper activities associated with infractions within or through the agency;

- Mechanisms for reporting violations of agency/center privacy-protection policies; and
- The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

P. INDIANA OPEN DOOR LAW AND ACCESS TO PUBLIC RECORDS ACT

It is the intent of the Indiana Open Door Law that the official actions of public agencies should be conducted openly, unless otherwise expressly provided by statute, in order that citizens may be fully informed.

It is the intent of the Indiana Access to Public Records Act to permit citizens to have broad and easy access to public documents. By providing the public with the opportunity to review and copy public documents, the citizens have the opportunity to obtain information relating to government and to more fully participate in the government process. The IIFC will conduct business in accordance with the Indiana Access Public Records Act (IC 5-14-3) and will allow access to records and documents consistent with its requirements and exceptions. Inquiries about the access to public records relating to IIFC data and documents should be addressed to the IIFC Executive Director.

If a request for disclosure of a public record under the Indiana Access to Public Records Act is received by IIFC, (including a request for ISE-SAR information posted to the shared space), such a public record may be disclosed to a member of the public only if the information is defined by law to be a public record or otherwise appropriate for release under the Indiana

Access to Public Records Act and if such document is not exempt from disclosure by law. Such information may be disclosed only in accordance with applicable Indiana law.

The requesting individual to whom a record has been disclosed or withheld, will be given a written reply which will delineate the records provided and the reasons for non-disclosure of any requested records which are denied by the IIFC. The individual will be informed of the procedure for filing a complaint with the Indiana Public Access Counselor or court if access to the record was denied.

If an individual has complaints or objections to the accuracy or completeness of ISE-SAR information about him or her that is alleged to be held by the IIFC, the IIFC, as appropriate, will inform the individual of the procedure for submitting complaints or requesting corrections. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

Appendix A- Terms and Definitions

28 C.F.R. Part 23 – Section 28 Part 23 of the Code of Federal Regulations governs Criminal Intelligence Offices which receive federal funding to operate.

Access - Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only and read/write access.

With regard to the ISE, access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

Acquisition - The means by which an ISE participant obtains information through the exercise of its authorities, for example, through human intelligence collection or from a foreign partner. For the purposes of this definition, acquisition does not refer either to the obtaining of information widely available to other ISE participants through, for example, news reports, or to the obtaining of information shared with them by another ISE participant who originally acquired the information.

Agency - Agency refers to the Indiana Intelligence Fusion Center and all agencies that access, contribute, and share information in the Indiana Intelligence Fusion Center's justice information system.

ARIES ESAR - ARIES ESAR is a raw informational report electronically submitted to IIFC by a criminal justice officer, based on his or her training and experience, of suspicious behavior that is indefinable at the moment but warrants further inquiry as a potential criminal/terrorist threat. The ARIES ESAR will be shared with other criminal justice agencies for criminal justice purposes without any other procedural approval process.

Audit Trail - Audit trail is a generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc.

Audit trails are a fundamental part of computer security, used to trace (usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authentication - Authentication is the process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are

digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords.

Authorization - The process of granting a person, computer process, or device with access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access that is verified through Authentication. See Authentication.

Biometrics - Biometrics methods can be divided into two categories: physiological and behavioral. Implementations of the former include face, eye (retina or iris), finger (fingertip, thumb, finger length or pattern), palm (print or topography), and hand geometry. The latter includes voiceprints and handwritten signatures.

Center - Center refers to the Indiana Intelligence Fusion Center.

Civil Liberties - Civil liberties are fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights, the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference. Generally, the term "civil rights" involves positive (or affirmative) government action, while the term "civil liberties" involves restrictions on government.

Civil Rights - The term "civil rights" refers to governments' role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed on government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.

Confidentiality - Confidentiality is closely related to privacy but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for and to protect and preserve the privacy of others. See Privacy.

Computer Security – The protection of information assets through the use of technology, processes, and training.

Credentials - Information that includes identification and proof of identification that is used to gain access to local and network resources. Examples of credentials are user names, passwords, smart cards, and certificates.

Data - Elements of information.

Data Breach – The unintentional release of secure information to an untrusted environment.

Data Protection –Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

Disclosure - The release, transfer, provision of access to, sharing, publication, or divulging of personal information in any manner—electronic, verbal, or in writing—to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

ESAR - ESAR is a legacy IIFC data system allowing Indiana criminal justice agencies to submit to the IIFC suspicious activity reports, raw information, electronically via the ARIES client. The ARIES ESAR is a raw informational report electronically submitted by a criminal justice officer, based on their training and experience, of suspicious behavior that is indefinable at the moment but warrants further inquiry as a potential criminal/terrorist threat.

Fair Information Practice Principles - The Fair Information Practice Principles (FIPPs) are a set of eight principles rooted in the Privacy Act of 1974. Under the Homeland Security Act of 2002, DHS has implemented these as the basis for privacy compliance policies and procedures governing the use of personally identifiable information. Some of the individual principles may not apply in all instances of integrated justice system. See Appendix F for **DHS Security Privacy Police Guidance Memorandum.**

The eight FIPPs are:
1. Transparency
2. Individual Participation
3. Purpose Specification Principle
4. Data Minimization
5. Use Limitation
6. Data Quality and Integrity
7. Security
8. Accountability and Auditing

Fusion Center - A collaborative effort of two or more agencies that provide resources, expertise, and information to a designated government agency or agency component with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity

Homeland Security Information - As defined in Section 892(f)(1) of the Homeland Security Act of 2002 and codified at 6 U.S.C. § 482(f)(1), homeland security information means any information possessed by a federal, state, or local agency that (a) relates to a threat of terrorist activity; (b) relates to the ability to prevent, interdict, or disrupt terrorist activity; (c) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (d) would improve the response to a terrorist act.

IIFC Personnel - IIFC personnel may include state employees, state agency contractors or subcontractors, and federal, state or local agency detailees assigned to the IIFC.

Information - information includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies may be categorized in general areas, including, but not limited to, general data, tips and leads data, suspicious activity reports, criminal intelligence information, intelligence information, or investigatory records.

Information Quality - Information quality refers to various aspects of the information; the accuracy and validity of the actual values of the data, data structure, and database/data repository design. Traditionally, the basic elements of information quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, information quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy.

ISE-SAR - A suspicious activity report (SAR) that has been determined, pursuant to a two-part process, to have a potential terrorism nexus. ISE-SAR business rules will serve as a unifying process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.

Intelligence (Criminal) – means data which has been evaluated to determine that it: (i) is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria.

Law - As used by this policy, law includes any local, state, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

Law Enforcement Information - For purposes of the ISE, law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both (a) related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

Lawful Permanent Resident – A foreign national who has been granted the privilege of permanently living and working in the United States.

Logs - See Audit Trail. Logs are a necessary part of an adequate security system because they are needed to ensure that data is properly tracked and that only authorized individuals are getting access to the system and the data.

Metadata - Data that provides information about other data.

Need to Know – mean the necessity to obtain or receive criminal intelligence information in the performance of official responsibilities as a law enforcement or criminal justice agency or authority.

Permissions – Authorization to perform operations associated with a specific shared resource, such as a file, a directory, or a printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

Personal Information - Information which can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in an activity or incident potentially related to terrorism.

Personally Identifiable Information (PII) - PII is one or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to specify a unique individual. The pieces of information can be:

- Personal characteristics (such as height, weight, gender, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, biometrics information such as fingerprints, DNA, and retinal scans).
- A unique set of numbers of characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Automated Integrated Fingerprint Identification Systems [AIFIS] identifier, or booking or detention system number)
- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).
- Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

Persons - Executive Order 12333 defines "United States persons" as United States citizens, aliens known by the intelligence agency concerned to be permanent resident aliens, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. For the intelligence community and for domestic law enforcement agencies, "persons" means United States citizens and lawful permanent residents.

Privacy - Privacy refers to individuals' interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the

right to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Policy - A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personal information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, disclosure, and access. The purpose of the privacy policy is to articulate that the agency/center will adhere to those legal requirements and agency/center policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

Privacy Protection - This is a process of maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

Protected Information - Protected information includes personal data about individuals that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the Indiana Constitution; applicable federal statutes and regulations, such as civil rights laws and 28 C.F.R. part 12; applicable state constitutions; and applicable state and local laws and ordinances.

Public -
Public includes:

- Any person and any for-profit or nonprofit entity, organization, or association;
- Any governmental entity for which there is no existing specific law authorizing access to the agency's/center's information;
- Media organizations; and
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

Public does not include:

- Employees of the agency;
- People or entities, private or governmental, who assist the agency/center in the operation of the justice information system; and
- Public agencies whose authority to access information gathered and retained by the agency/center is specified in law.

Record - Any item, collection, or grouping of information that includes personally identifiable information and is maintained, collected, used, or disseminated by or for the collecting agency or organization.

Redress - Internal procedures to address complaints from persons regarding protected information about them that is under the IIFC's control.

Retention - Refer to Storage.

Right to Know – means the legal authority to obtain or receive criminal intelligence information pursuant to court order, statute or decisional law.

Right to Privacy – The right to be left alone, in the absence of some reasonable public interest in gathering, retaining, and sharing information about a person's activities. Invasion of privacy can be the basis for a lawsuit for damages against the person or entity violating a person's privacy.

Role-Based Access - A type of access that uses roles to determine rights and privileges. A role is a symbolic category of users that share the same security privilege.

Security - Security refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

Shared Space - A networked data and information repository that is under the control of submitting agencies and which provides terrorism-related information, applications, and services to other ISE participants.

Sharing - Refers to the act of one ISE participant disseminating or giving homeland security information, terrorism information, or law enforcement information to another ISE participant.

Source Agency - Source agency refers to the agency or entity that originates SAR (and, when authorized, ISE-SAR) information.

Storage - In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:

- Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This meaning is probably more common in the IT industry than meaning 2.

- In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory or RAM) and other "built-in" devices such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

- Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

- With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism-related information, to include homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland by both the originator of the information and any recipient of the information.

Submitting Agency - Submitting agency refers to the agency or entity providing ISE-SAR information to the shared space.

Suspicious Activity - Defined in the ISE-SAR Functional Standard (Version 1.5) as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyber- attacks, testing of security, etc.

Suspicious Activity Reports (SARs) - Official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. Suspicious activity report (SAR) information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

Terrorism Information - Consistent with Section 1016(a)(4) of IRTPA, all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign or international terrorist groups or individuals or of domestic groups or individuals involved in transnational terrorism, (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations, (c) communications of or by such groups or individuals, or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Terrorism-Related Information - In accordance with IRTPA, as recently amended by the 9/11 Commission Act enacted on August 3, 2007 (P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also Information Sharing Environment Implementation Plan (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of "terrorism information," as defined in IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information:" (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information includes intelligence information.

Weapons of Mass Destruction (WMD) information as a fourth (third statutory) category of ISE information is not called for in P.L. 110-53. Rather, it amends the definition of terrorism information to include WMD information and then defines that term. WMD information probably should not technically be cited or referenced as a fourth category of information in the ISE.

Tips and Leads Information or Data - Uncorroborated report or information generated from inside or outside the agency that alleges or indicates some form of possible criminal activity. Tips and leads can also be referred to as suspicious incident reports (SIRs), suspicious activity reports (SARs), and/or field interview reports (FIRs). Tips and leads information does not include incidents that do not have an offense attached, criminal history records, or Computer Aided Dispatch (CAD) data.

A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information has some suspicion or mere suspicion attached to it, but without further inquiry or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of no use to law enforcement and being extremely valuable depending on whether time and resources are available to determine its meaning.

Tips and leads information is maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

User Agency - User agency refers to the agency or entity authorized by the submitting agency, or other authorized agency or entity, to access ISE-SAR information in the shared space(s), and which may include analytical or operational component(s) of the submitting or authorizing agency or entity.

THE REMAINDER OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY

Appendix C

Receipt of IIFC Privacy Policy
By IIFC and Non-IIFC Personnel

My signature below indicates that I have been provided a copy, have read and that I understand the Indiana Intelligence Fusion Center Privacy Policy. I understand that the Privacy Policy applies to me and that its violation may serve as a basis for a disciplinary action, up to and including dismissal.

Signature: _____

Printed Name: _____

Date Signed: _____

Appendix E

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
privacy@dhs.gov
www.dhs.gov/privacy

December 29, 2008

PRIVACY POLICY GUIDANCE MEMORANDUM

Memorandum Number: 2008-01

FROM: Hugo Teufel III
Chief Privacy Officer

SUBJECT: The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security

I. PURPOSE

This Memorandum memorializes the Fair Information Practice Principles (FIPPs) as the foundational principles for privacy policy and implementation at the Department of Homeland Security (DHS).

II. AUTHORITY

The FIPPs are a set of eight principles that are rooted in the tenets of the Privacy Act of 1974.[1] The Chief Privacy Officer's authority to use these principles as the framework for privacy policy at DHS is based upon Sections 222 (a)(1) and (a)(2) of the Homeland Security Act of 2002, as amended,[2] which authorize the Chief Privacy Officer to assume primary responsibility for DHS privacy policy, including (1) assuring that the use of technologies sustains and does not erode, privacy protections relating to the use, collection, and disclosure of personal information; and (2) assuring that personal information contained in DHS Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act.

III. POLICY

The FIPPs form the basis of the Department's privacy compliance policies and procedures governing the use of personally identifiable information (PII). These principles are: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing. DHS uses the

[1] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.
[2] Homeland Security Act of 2002, as amended, 6 U.S.C. § 142.

FIPPs to assess and enhance privacy protections by analyzing the nature and purpose of the collection of PII to fulfill DHS's mission and how the Department can best provide privacy protections in light of these principles.

IV. BACKGROUND

The FIPPs are a widely accepted framework that is at the core of the Privacy Act of 1974 and is mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The concept of defining principles to be used in the evaluation and consideration of systems, processes, or programs that impact individual privacy is not a new one. In his seminal work, *Privacy and Freedom*, published in 1967, Professor Emeritus Alan Westin identified a number of "criteria for weighing conflicting interests."[3] A few years later, an advisory committee of the U.S. Department of Health, Education, and Welfare (HEW) proposed similar principles.

The HEW advisory committee's report, entitled, *Records, Computer, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*,[4] was the result of the committee's look at the impact of computerization of information on privacy and included recommendations on developing policies that would allow the benefits of computerization to go forward, but at the same time provide safeguards for personal privacy. The backdrop surrounding the HEW report and the Privacy Act included several years of intense Congressional hearings examining the surveillance activities of the Nixon and J. Edgar Hoover era and the post-Watergate support for government reform. Flowing from the numerous abuses of power uncovered by Congress and the media during the early 1970's, the Privacy Act set out a comprehensive regime limiting the collection, use and dissemination of personal information held by government agencies. The Privacy Act also established penalties for improper disclosure of personal information and gave individuals the right to gain access to their personal information held by Federal agencies.

A number of European countries also began to build upon the HEW principles and individually enacted omnibus data protection laws. In 1980, the international Organization of Economic Cooperation and Development (OECD) codified its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.[5] In 1995, a variation of these principles became the basis of the European Union Data Protection Directive. The FIPPs have also been agreed upon by member countries, including the United States, through a consensus and formal ratification process and form the basis of many modern international privacy agreements and national laws.

---

[3] These principles were included in chapter 14 of *Privacy and Freedom*, entitled "Restoring the Balance of Privacy in America." The Privacy Office has not adopted the notion of balancing privacy against other values because that paradigm results in a zero-sum outcome and privacy often is diminished at the expense of security.

[4] http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm

[5] http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

As recently as 2004, the FIPPs were championed again by the United States in the development of the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.[6] The FIPPs principles have also formed the basis of many individual laws in the United States, at the both Federal and state levels, including the Fair Credit Reporting Act, the Right to Financial Privacy Act, the Electronic Communications Privacy Act, the Video Privacy Protection Act, and the Children's Online Privacy Protection Act. Many states have incorporated these principles in their own state laws governing public records and in some instances private sector data as well. A number of private and not-for-profit organizations have also incorporated these principles into their privacy policies.

Section 222 of the Homeland Security Act of 2002, as amended,[7] which is the basis for the authorities and responsibilities of the DHS Chief Privacy Officer, also recognizes the significance of the FIPPs. This section calls on the Chief Privacy Officer to "assur[e] that personal information contained in Privacy Act systems of records is handled in full compliance with *fair information practices* as set out in the Privacy Act of 1974" (emphasis added). . Pursuant to Section 222, the Privacy Office has used the FIPPs to assess privacy when conducting Privacy Impact Assessments, issuing System of Records Notices, and developing privacy policy for the Department. The FIPPs provide the foundation of all privacy policy development and implementation at the Department and must be considered whenever a DHS program or activity raises privacy concerns or involves the collection of personally identifiable information from individuals, regardless of their status.

V. THE FAIR INFORMATION PRACTICE PRINCIPLES

- Transparency: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).
- Individual Participation: DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.
- Purpose Specification: DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

---

[6] http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1

[7] Homeland Security Act of 2002, as amended, 6 U.S.C. § 142.

- Data Minimization: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
- Use Limitation: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.
- Data Quality and Integrity: DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
- Security: DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- Accountability and Auditing: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

The DHS Privacy Office, therefore, has adopted the FIPPs as its privacy policy framework and seeks to apply them to the full breadth and diversity of DHS programs and activities. Any questions regarding the application or implementation of these principles should be directed to the DHS Privacy Office at privacy@dhs.gov or (703) 235-0780.